(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
15 janvier 2004 (15.01.2004)

PCT

(10) Numéro de publication internationale
WO 2004/006498 A2

(51) Classification internationale des brevets[7] : H04L 9/32

(21) Numéro de la demande internationale :
PCT/FR2003/002074

(22) Date de dépôt international : 4 juillet 2003 (04.07.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
02/08418 4 juillet 2002 (04.07.2002) FR

(71) Déposant *(pour tous les États désignés sauf US)* : ERA-COFA SA [FR/FR]; 36, rue du Bois, F-44510 Le Pouliguen (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : SUANEZ, Roger [FR/FR]; 36, rue du Bois, F-44510 Le Pouliguen (FR). ETIENNE, Patricia [FR/FR]; 36, rue du Bois, F-44510 Le Pouliguen (FR).

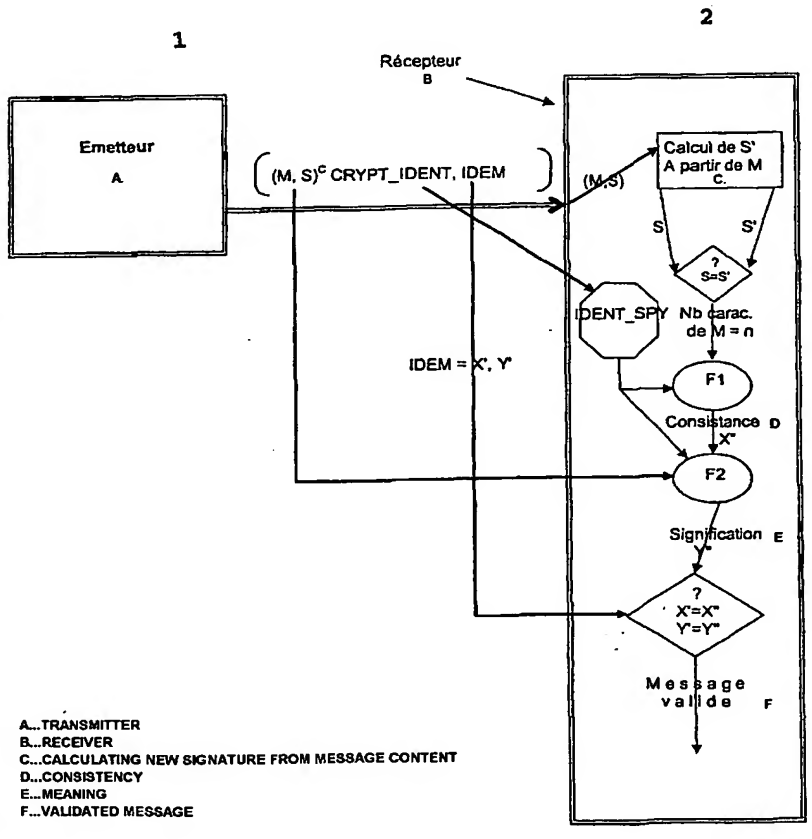
(74) Mandataire : LEPEUDRY, Thérèse; Cabinet Lepeudry, 43, rue de la Brèche aux Loups, F-75012 Paris (FR).

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

[Suite sur la page suivante]

(54) Title: METHOD, SYSTEM AND COMPUTERIZED MEDIUM FOR MAKING SECURE MESSAGE TRANSMISSION

(54) Titre : PROCEDE, SYSTEME ET SUPPORT INFORMATIQUE DE SECURISATION DE TRANSMISSION DE MESSAGES



(57) **Abstract:** The invention concerns a method for making secure message transmission comprising a step which consists in transmission of the message and its signature by the transmitter (1) as well as an identification information of the transmitter (CRYPTIDENT) and a supplementary information derived from the message (IDEM), and the receiver (2) likewise determines an information derived from the content of the received message and compares it to the transmitted corresponding information (IDEM) to validate the message in case of conformity.

(57) **Abrégé :** Le procédé de sécurisation de la transmission de message comporte une étape de transmission du contenu du message et de sa signature par l'émetteur (1) ainsi que d'une information d'identification de l'émetteur (CRYPTIDENT) et d'une information supplémentaire découlant du message (IDEM), et le récepteur (2) détermine de même une information découlant du contenu du message reçu et la compare à l'information homologue transmise (IDEM) pour valider le message en cas de coïncidence.

WO 2004/006498 A2

(84) **États désignés** *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *sans rapport de recherche internationale, sera republiée dès réception de ce rapport*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

Procédé, système et support informatique de sécurisation de transmission de messages

La présente invention concerne la sécurisation de la transmission de messages.

Il est connu, dans la sécurisation de message, de déterminer une signature d'un message et de transmettre celle-ci accolée au message pour permettre à un dispositif récepteur, possédant une clé appairée à une clé ayant permis la génération de signature du message, soit de déchiffrer le message signé soit de calculer, à partir de la clé appairée, une autre signature et de la comparer à la signature reçue. Par clé appairée, il faut comprendre soit une clé publique associée à une clé privée d'un algorithme de chiffrement à clé publique, soit deux clés secrètes connues, l'une, d'une première entité, permettant le chiffrement d'un message envoyé, l'autre pour le déchiffrement d'un message reçu d'une autre entité disposant de l'autre clé permettant le déchiffrement des messages reçus de la première entité ou le chiffrement des messages émis vers la première entité.

Ces techniques de chiffrement des communications sous protocole sécurisé par cryptographie asymétrique (par exemple publique) ou symétrique présentent l'inconvénient que, à la fin d'un cycle de transport ou transfert, les contenus dématérialisés et signés ne sont pas toujours au rendez-vous et l'organisme récepteur n'est pas en mesure de certifier que le message reçu correspond parfaitement à celui émis et que, entre autres, l'autorité qui s'auto-certifie ne peut pas valablement prouver l'intégrité des contenus lorsqu'ils ont fait l'objet d'altération accidentelle ou préméditée durant un cycle de leur transfert. En effet, il peut arriver que le message et la signature soient, fortuitement ou volontairement, tous deux

altérés de façon coordonnée pour que l'altération ne puisse pas être détectée en fin de cycle d'auto-certification.

Les inventeurs ont en outre songé au fait que le problème de risque d'altération d'un message découle du fait que l'émetteur en perd le contrôle d'accès. Or, ce même problème se pose dans le cas du stockage de données dans un ordinateur personnel, à accès mal contrôlé, ou dans tout autre moyen de stockage local ou distant.

L'accès au moyen de stockage peut donc s'effectuer par une liaison interne de courte portée, vers un disque dur de l'ordinateur personnel, et alors la liaison se trouve protégée, lors du transfert, par le fait qu'elle est interne et que l'utilisateur est présent, mais il convient, après stockage, de protéger l'accès au disque dur, et donc en particulier cette liaison.

Lorsque le moyen de stockage est distant, l'émetteur y accède par une ligne dédiée ou, en général, par un réseau informatique local ou général, par exemple l'Internet. En pareil cas, le message peut être détourné ou modifié par un tiers lors de sa transmission.

L'invention vise donc à améliorer l'efficacité de la vérification d'intégrité d'un bloc de données dont le créateur a perdu le contrôle d'accès du fait d'une émission. Les données peuvent se présenter sous une forme quelconque, par exemple électronique, en mémoire optique, ou encore imprimées.

A cet effet, l'invention concerne tout d'abord un procédé de sécurisation de la transmission d'un message d'un émetteur à un récepteur, dans lequel l'émetteur élabore et intègre au message une signature pour former un message signé, caractérisé par le fait qu'il comporte les étapes suivantes :

- l'émetteur associe au message signé des informations de contrôle en émission, découlant du message signé selon une loi déterminée, et
- l'émetteur élabore et émet, à destination du récepteur, des données représentant le message signé et les informations de contrôle en émission,

et le récepteur :

- reçoit les dites données transmises,
- détermine selon ladite loi des informations de contrôle en réception découlant du message reçu, et
- compare les informations de contrôle en réception avec les informations de contrôle en émission, pour valider le message reçu en cas de coïncidence.

Comme évoqué ci-dessus, le terme « message » doit être compris comme désignant tout ensemble de données transmis, cet ensemble de données n'étant pas nécessairement transmis sur une liaison d'un réseau informatique, et pouvant être de format quelconque et en particulier être exempt d'adresse d'émetteur et de récepteur.

Les informations de contrôle permettent ainsi de contrôler efficacement le contenu utile du message et au besoin aussi la signature. L'émetteur et le récepteur peuvent être des opérateurs humains ou des équipements de traitement de l'information. On notera que les informations de contrôle en émission peuvent être transmises de façon séparée du message.

Dans une forme de réalisation préférée, la dite loi met en œuvre une fonction mathématique.

Le traitement peut ainsi s'effectuer par blocs de bits représentant par exemple un caractère du message. Un tel traitement des bits, parallèle et combiné, offre beaucoup plus de combinaisons qu'une fonction logique, à traitement série, comme par exemple une fonction OU exclusif. Le

traitement par blocs est en outre plus rapidement exécuté dans une unité centrale classique, prévue pour uniquement des fonctions logiques et donc incapable de traiter indépendamment en parallèle plusieurs bits.

De façon préférée, l'émetteur élabore et transmet en outre des informations d'identification de l'émetteur ayant servi à personnaliser ladite loi, et le récepteur personnalise de même la loi, d'après les informations d'identification de l'émetteur reçues, pour déterminer les informations de contrôle en réception.

L'état civil de l'émetteur représente ainsi une clé supplémentaire de contrôle.

Avantageusement, l'émetteur établit la dite loi pour que les informations de contrôle en émission soient représentatives d'au moins un type d'informations choisi parmi le groupe formé par des informations de consistance et des informations de signification du message.

Ainsi, la structure du message et/ou la signification des informations qu'il contient peut être vérifiée car elle est traduite dans les informations de contrôle.

Les informations de consistance du message peuvent par exemple être déterminées par un premier quotient provenant d'une division des informations d'identification de l'émetteur par un nombre de caractères contenus dans le message.

En pareil cas, un premier reste obtenu par la dite division peut être lui-même divisé par un nombre premier, pour obtenir un deuxième quotient et un deuxième reste, le deuxième reste étant ajouté à une constante pour obtenir un nombre de caractères prédéterminé, de consistance du message, après conversion dans une base choisie parmi une pluralité de bases de conversion.

Le reste du deuxième quotient peut en outre être divisé par un nombre premier pour obtenir un troisième

quotient associé à un troisième reste dont la valeur est ajoutée à une valeur constante, pour obtenir les informations de consistance du message.

Le nombre premier est par exemple 46027 et la constante est par exemple 4623.

Les informations de consistance du message sont de préférence représentées par des caractères dont le nombre est inférieur à un seuil représentant un pourcentage déterminé par rapport à une taille des données transmises.

Les informations de signification du message sont par exemple déterminées par sommation d'un nombre déterminé de caractères alphanumériques du message, chaque caractère alphanumérique ayant pour valeur le double d'une valeur ASCII représentative du caractère considéré, diminuée d'une valeur ASCII représentative d'un caractère adjacent, la somme résultante servant de diviseur d'un dividende, constitué par les informations d'identification de l'émetteur, pour obtenir les informations de signification du message.

Les informations de signification du message sont de préférence représentées par des caractères dont le nombre est inférieur à un seuil représentant un pourcentage déterminé par rapport à une taille des données transmises.

Les informations d'identification de l'émetteur sont par exemple obtenues :

par une étape de transcodage de chaînes, de tailles déterminées, de caractères alphanumériques représentant des rubriques à protéger, fournissant un premier ensemble de résultats intermédiaires ayant chacun un nombre déterminé de chiffres, et

une étape de transformation du premier ensemble de résultats intermédiaires, par un algorithme de transformation choisi aléatoirement parmi une pluralité utilisant chacun une base de caractères alphanumériques

particulière à l'algorithme considéré, pour obtenir un résultat final après conversion, par une matrice de conversion, des caractères de la base alphanumérique de l'algorithme choisi en des caractères à valeurs numériques d'une base prédéterminée.

Les informations d'identification de l'émetteur sont de préférence transmises sous forme cryptée, en transformant les informations d'identification de l'émetteur, en base déterminée, en un résultat crypté, à nombre déterminé de chiffres exprimés dans une base mathématique choisie aléatoirement parmi une pluralité de bases de conversion pour obtenir un identifiant crypté de l'émetteur dans lequel des informations, d'identification de la base mathématique choisie, sont insérées à un rang variable spécifié par un pointeur inséré à un rang pour lequel le récepteur dispose d'informations pour le déterminer.

En pareil cas, le rang des informations d'identification de la base mathématique choisie est par exemple défini par un quotient entier obtenu par division d'une valeur particulière, associée par une table au pointeur, par un nombre spécifiant la taille de la pluralité d'algorithmes.

Le rang du pointeur est par exemple inséré à un rang calculé en prenant la somme, modulo 9, de codes ASCII d'un dit résultat intermédiaire représentant des termes spécifiant une fonction mathématique déterminant les informations d'identification de l'émetteur.

Dans un mode de mise en œuvre, le récepteur :

calcule la somme des codes ASCII d'au moins un bloc de données d'une dite rubrique alphanumérique, reçu dans les informations d'identification de l'émetteur,

- exprime la dite somme en modulo 9, pour déterminer le rang du pointeur,
- lit le dit pointeur reçu, et

- calcule le rang des informations d'identification de la base mathématique choisie, en divisant la valeur particulière, associée au pointeur, par la valeur représentant la taille de la pluralité d'algorithmes, exprimées en base prédéterminée, et
- exploite les informations cryptées reçues après en avoir éliminé les informations d'identification de la base mathématique choisie et le pointeur.

Les données représentant le message peuvent être transmises au récepteur à travers un système de stockage de données.

En pareil cas, le récepteur peut être aussi l'émetteur, c'est-à-dire que le créateur des données utiles peut les relire ultérieurement, après stockage local ou distant, et en vérifier l'intégrité.

L'invention concerne aussi un système de sécurisation pour la mise en œuvre du procédé de l'invention, comprenant un émetteur associé à un récepteur, l'émetteur étant agencé pour élaborer et intégrer au message une signature pour former un message signé, caractérisé par le fait que :

l'émetteur comporte :

- des moyens pour élaborer et associer, au message signé, des informations de contrôle en émission, découlant du message signé selon une loi déterminée, et
- des moyens d'émission, à destination du récepteur, de données représentant le message signé et les informations de contrôle en émission,

et le récepteur comporte :

- des moyens de réception des dites données transmises,
- des moyens de détermination, selon ladite loi, d'informations de contrôle en réception découlant du message reçu, et

- des moyens de comparaison des informations de contrôle en réception avec les informations de contrôle en émission, pour valider le message reçu en cas de coïncidence.

Les moyens d'émission sont en outre de préférence commandés par des moyens d'élaboration d'informations d'identification de l'émetteur ayant servi à personnaliser ladite loi, et le récepteur comporte des moyens de personnalisation de même de la loi, d'après les informations d'identification de l'émetteur reçues par les moyens de réception, commandant les moyens de détermination des informations de contrôle en réception.

L'émetteur est de préférence agencé pour que la dite loi fasse que les informations de contrôle en émission soient représentatives d'au moins un type d'informations choisi parmi le groupe formé par des informations de consistance et des informations de signification du message.

Les divers moyens ci-dessus de l'émetteur et du récepteur peuvent être des éléments matériels ou circuits câblés pour effectuer leur fonction, et/ou des éléments logiciels tournant sur de tels éléments matériels dédiés ou, commodément, sur une unité centrale arithmétique utilisée en partage de temps entre ces fonctions et éventuellement d'autres fonctions externes à l'invention. Chaque fonction selon l'invention peut donc se présenter sous la forme d'un logiciel stocké dans un support informatique de mémoire fixe ou amovible, par exemple un disque dur, une disquette, un CD ROM, une carte à puce ou autre, situé à proximité de l'émetteur ou du récepteur ou bien distant et accessible à ceux-ci. La carte à puce peut en outre comporter tout ou partie des moyens de traitement mettant en œuvre les logiciels.

L'invention concerne enfin un support de données contenant un ensemble de logiciels de commande d'un système

informatique pour la mise en œuvre du procédé de l'invention, l'ensemble de logiciels comportant au moins l'un parmi les deux sous-ensembles suivants :

un premier sous-ensemble, destiné à l'émetteur, contenant un logiciel pour commander au système d'associer au message signé des informations de contrôle en émission, découlant du message signé selon une loi déterminée, et un logiciel pour commander d'élaborer et d'émettre, à destination du récepteur, des données représentant le message signé et les informations de contrôle en émission, et

un second sous-ensemble, destiné au récepteur, contenant un logiciel de réception des dites données transmises, un logiciel de détermination, selon ladite loi, des informations de contrôle en réception découlant du message reçu, et un logiciel de comparaison des informations de contrôle en réception avec les informations de contrôle en émission, pour valider le message reçu en cas de coïncidence.

Le premier sous-ensemble peut en outre contenir un logiciel d'élaboration et de transmission en outre d'informations d'identification de l'émetteur ayant servi à personnaliser ladite loi, et le second sous-ensemble contient un logiciel de personnalisation de même de la loi, d'après les informations d'identification de l'émetteur reçues, pour déterminer les informations de contrôle en réception.

La dite loi peut être établie pour que les informations de contrôle en émission soient représentatives d'au moins un type d'informations choisi parmi le groupe formé par des informations de consistance et des informations de signification du message.

Le support de données peut consister en une carte à puce.

L'invention sera mieux comprise à l'aide de la description suivante d'un mode préféré de mise en œuvre du procédé de l'invention, en référence au dessin annexé, dans lequel :

- la figure 1 représente globalement les moyens nécessaires à la mise en œuvre du procédé de l'invention, constitués d'un émetteur et d'un récepteur reliés par une ligne de transmission de messages,
- la figure 2 représente schématiquement une vue de détail des opérations qui se déroulent au niveau de l'émetteur et du récepteur,
- la figure 3 représente schématiquement une vue de détail des informations d'élaboration du chiffrement de protection des contenus des messages qui se déroulent au niveau de l'émetteur, et
- la figure 4 représente des étapes de détermination d'une information d'identification de l'émetteur IDENT_SPY pour utilisation dans les opérations de la figure 2 à partir de l'information d'identification cryptée.

En référence aux figures 1 et 2, dans une transmission classique de messages d'informations entre deux terminaux informatiques respectivement un émetteur 1 et un récepteur 2 à travers une ligne de communication. L'émetteur 1 lit, à une étape 101 (fig. 2), une clé secrète pour effectuer, sur le contenu du message M, un calcul d'une signature S à une étape 103 qui est ensuite adjointe au contenu du message pour former un message signé, subissant éventuellement une opération de chiffrement C, étape 103, le message signé chiffré $(M,S)^c$ étant ensuite transmis, à une étape 105, au récepteur 2 par la ligne de communication.

Ensuite le récepteur 2, par utilisation d'un algorithme de déchiffrement, symétrique ou asymétrique, étape 202 après lecture d'une clé publique, étape 201, déchiffre si nécessaire le message signé chiffré, pour en extraire le

contenu utile du message et la signature reçue. Le récepteur 2 effectue, sur ce contenu, le même calcul que celui effectué par l'émetteur 1, pour déterminer localement une nouvelle signature S' qu'il compare à la signature S reçue. En cas d'égalité lors de la comparaison, le récepteur 2 considère que le message reçu, et donc le contenu utile, correspond à celui émis.

Toutefois ce processus n'est pas infaillible car, par exemple, le récepteur 2 ne détectera pas qu'un fraudeur a inversé les positions de caractères du contenu du message, car la signature ne le détecte pas toujours, ou encore qu'il a reçu, du fraudeur, un message à contenu déterminé par ce dernier mais valablement signé, éventuellement en substitution d'un message signé authentique.

Selon le procédé illustré plus en détails à la figure 2, l'émetteur 1 calcule en plus, à une étape 104, des informations de signature en émission IDEM, découlant du message selon une loi déterminée. Dans cet exemple, l'émetteur 1 calcule en outre, dans une base de calcul d'identité Y déterminée de façon aléatoire, des informations d'identification de l'émetteur, IDENT_SPY, qui sont éventuellement cryptées en CRYPT_IDENT, auxquelles l'émetteur 1 ajoute des informations d'identification de la base Y. L'ensemble de ces informations, IDEM et IDENT_SPY ou CRYPT_IDENT, est ensuite transmis au récepteur 2.

L'émetteur 1 associe ainsi au message signé des informations IDEM de contrôle en émission, découlant du message signé selon la loi déterminée, et l'émetteur 1 élabore et émet, à destination du récepteur 2, des données représentant le message signé et les informations de contrôle en émission IDEM, ainsi que, dans cet exemple, les informations d'identification de l'émetteur, IDENT_SPY, qui personnalisent la loi.

A réception de ces informations, le récepteur 2 va tout d'abord, si nécessaire, déchiffrer (C^{-1}) la partie chiffrée du message puis calculer une signature S' d'après le contenu du message M déchiffré et la comparer avec la signature reçue S, pour vérifier qu'elles sont identiques.

Dans le cas où cette comparaison préalable est positive, le récepteur 2 détermine, selon ladite loi, des informations IDEM' de contrôle en réception découlant du message reçu, et il compare les informations de contrôle en réception IDEM' avec les informations de contrôle en émission IDEM, pour valider le message reçu en cas de coïncidence.

La dite loi met ici en œuvre une fonction mathématique.

Le récepteur 2 poursuit ici son processus de validation du message en déterminant, à partir des informations d'identification de l'émetteur IDENT_SPY cryptées CRYPT_IDENT, étape 203, celles, indiquées plus haut, qui permettent de retrouver la base Y de calcul de la valeur d'informations d'identification de l'émetteur 1, c'est-à-dire le terminal ou son utilisateur, IDENT_SPY, constituées d'une suite de par exemple 11 à 12 chiffres ou caractères ayant chacun une valeur numérique particulière.

A une étape 204, les informations d'identification de l'émetteur 1, IDENT_SPY ou CRYPT_IDENT, sont ici combinées par le récepteur 2 à un nombre, préalablement relevé, de caractères alphanumériques constituant le message, pour en déduire des informations X'' de consistance du message en réception. Les informations d'identification de l'émetteur 1 IDENT_SPY sont aussi ici combinées à des valeurs ASCII représentatives de chacun des caractères du message pour en déduire des informations de signification (Y'') du message en réception. Le récepteur 2 compare alors, étape 205, les informations de consistance et de signification X'', Y'' calculées en réception, aux informations homologues X', Y'

reçues de consistance et de signification du message en émission, comprises dans les informations de contrôle en émission découlant du message IDEM.

Les références 101 à 105 et 201 à 205 désignent, outre les étapes indiquées, deux ensembles de blocs de calcul de traitement, de circuits matériels et/ou de logiciels de l'émetteur 1 et respectivement du récepteur 2, prévus pour exécuter les fonctions indiquées.

L'information de consistance du message en réception X'' est ici calculée par le récepteur 2 en appliquant l'algorithme suivant :

le récepteur 2 utilise ici un nombre représentant l'information d'identification de l'émetteur IDENT_SPY, dont chaque caractère représente une valeur particulière, et effectue une première division, en divisant ce nombre par une valeur d'un nombre représentant le nombre de caractères du message.

Un premier reste obtenu dans la première division est, dans une deuxième division, lui-même divisé par un nombre premier constitué, par exemple, par le nombre premier 46027.

Un deuxième reste obtenu dans la deuxième division est ajouté à ici la valeur 4623 pour s'assurer que le résultat est toujours compris entre des bornes de valeur permettant de coder ce résultat, dans l'une des bases de la pluralité de bases de conversion ou condensation, sous un nombre de caractères alphanumériques restreint, par exemple 3 caractères.

La pluralité de bases de conversion peut par exemple être constituée par des bases comprises entre la base 37 et la base 127. La base 82, valeur moyenne des bases contenues dans la plage d'étendue des caractères du code à barres 128, sert de référence d'évaluation de la robustesse moyenne de ce procédé contre la casse par force brutale.

L'annexe 1 représente la matrice de conversion bijective des caractères en base 37 dans la base décimale et vice-versa.

L'annexe 2 représente la matrice de la base de conversion 67 permettant la conversion des 67 caractères alphanumériques de la colonne b67 en chiffres de la base décimale représentés à la colonne b10 et vice-versa.

On notera que, si la base décimale constitue une base classique servant ici de référence, toute autre base de référence peut toutefois être utilisée.

Afin d'obtenir l'information de signification du message en réception Y'', le récepteur 2 utilise également ici l'information d'identification IDENT_SPY comme dividende pour diviser cette valeur par la somme d'un certain nombre d'éléments, à valeur numérique, correspondant chacun en propre à l'un, particulier, des caractères du message. Chaque élément a ici pour valeur le double de la valeur ASCII d'un caractère de rang k diminuée de la valeur ASCII du caractère suivant de rang k+1, selon un ordre de progression prédéterminé, dans un sens ou dans l'autre. Le reste ainsi obtenu est lui-même divisé par ici le nombre premier 46027, et le reste obtenu est ajouté à ici la valeur 4623 pour déterminer une valeur représentée dans l'une des bases choisies, par exemple en base 37 ou en base 67, sous forme de 3 caractères.

Les valeurs de consistance X'' et de signification Y'' calculées en réception sont comparées aux valeurs homologues X' et Y', transmises avec le message M ou séparément, ayant été calculées par l'émetteur 1. La valeur de signification Y', comme on le comprendra par l'exemple ci-après, est déterminée de telle façon que la valeur du nombre d'identification de l'émetteur IDENT_SPY, fixée pour limiter la capacité de registres mémoires, est étendue dans cet exemple entre 32259945714 et 32259948772 lorsqu'il est

divisé, par la première division, par le diviseur qui est constitué à partir de la valeur ASCII des caractères, ou à partir du nombre de caractères, comme on l'a expliqué précédemment et qui peut donc prendre une valeur comprise, dans cet exemple, entre 003210985 et 333210952.

Puis lorsque, par la deuxième division, on divise le premier reste, obtenu par la première division, par le nombre premier 46027, on obtient un second reste auquel il est ajouté la valeur constante 4623. On obtient, dans un premier cas, concernant la vérification de consistance du message, la valeur 4623 en base 10 qui, transformée en base 37, vaut « 3dz » et, en base 67, « 120 ». Dans un deuxième cas, concernant la signification du message, on obtient 50649 en base 10, ce qui, représenté en base 37, prend la valeur « Aax », et, en base 67, la valeur « bi£ ». Les trois informations (la première information, d'identification de l'émetteur CRYPT_IDENT, et les deuxième et troisième informations de consistance X' et de signification Y' du message) ainsi ajoutées ou associées au message, constituent, pour la première, une information qui se distingue indépendamment des deux suivantes.

La première information, d'identification de l'émetteur, CRYPT_IDENT, est obtenue d'un bloc de longueur prédéterminée, encore appelé ici troncature, de plusieurs caractères ici de poids forts, parmi lesquels se trouve placé, à un rang tiré aléatoirement, un caractère représentant la base mathématique Y d'expression du résultat du calcul.

La première information, d'identification de l'émetteur, CRYPT_IDENT, constitue un premier bloc formant un condensé identitaire, d'une personne physique ou morale ou d'un document ou d'un objet, obtenu par application d'un algorithme de calcul As tiré aléatoirement parmi une pluralité de taille s et dont les différents termes et

constantes de la fonction mathématique sont constitués de nombres convertis, exprimés en base déterminée, ici décimale, et provenant des différentes rubriques alphabétiques et numériques identifiant la personne morale, la personne physique, l'objet, le document ou l'information à authentifier dans la transmission.

La seconde information X' découle du contenu du document dématérialisé et fournit la preuve de sa consistance en vérifiant que le message contient bien les N caractères prévus et cette seconde information est exprimée dans cet exemple par la fonction (F1) :

$$\text{IDENT\_SPY MOD} \sum_{Ci=1}^{Ci=n} C_i \bmod 46027 + 4623 = X'$$

La troisième information Y' découle aussi du contenu du message et fournit la preuve de son sens ou de sa signification en reposant sur la valeur ASCII de chacun des caractères composant le message. Cette troisième information est obtenue dans cet exemple par la formule (F2) :

$$\text{IDENT\_SPY MOD} \sum_{Ci=1}^{Ci=n-1} (2\ \text{val ASCII}\ C_i - \text{val ASCII}\ C_{i+1}) \bmod 46027 + 4623 = Y'$$

Ces deux derniers résultats concaténés X', Y' forment un second bloc, ou troncature, de caractères de poids faibles, qui, concaténée à la première troncature d'identification de l'émetteur CRYPT_IDENT, est ici concaténée au message signé M,S. La première troncature, d'identification de l'émetteur, CRYPT_IDENT, confirme l'identité du signataire du message dématérialisé et déchiffré, la seconde troncature X', Y' permet sa validation ou sa répudiation en cas d'altération pour causes diverses du contenu.

Le système et procédé décrits peuvent être utilisés également pour des paiements électroniques effectués par titre au porteur pourvu d'une zone grattable ou autre

découvrant la seconde troncature X', Y' qui doit alors contenir un code aléatoire résultant du calcul effectué pour valider des références de chacun des titres.

Le principe d'élaboration d'un résultat de traitement, selon un exemple particulier, d'informations à protéger va maintenant être explicité en liaison avec les figures 3 et 4 pour permettre une meilleure compréhension de la présente invention.

Pour la clarté de l'exposé, sur l'organigramme d'étapes du procédé illustré par la figure 3, des blocs de calcul ou traitement effectuant les étapes respectives sont chacun dessinés sous une forme de plusieurs cadres élémentaires illustrant leur fonction, leur référence, avec une centaine 1, étant portée à côté.

Un premier résultat est élaboré, par un bloc de calcul 110 de l'émetteur 1, à partir de chaînes de caractères alphanumériques, ici des chaînes de caractères alphabétiques Ch1 à Ch4 et des chaînes de valeurs numériques Ch5 à Ch7, représentant des rubriques à protéger pour identifier des falsifications sur des informations ou des documents ou des identités de personnes physiques ou morales, ou d'objets.

Les chaînes Ch1 à Ch7 sont ensuite condensées, par un bloc de calcul 111, en une pluralité d'ici quatre résultats intermédiaires référencés 11, 12, 13, 14 comportant chacun un nombre p de chiffres déterminés, représentant des caractères et des valeurs numériques des chaînes Ch1 à Ch7, inférieurs ou égaux à la valeur de la base utilisée moins une unité, c'est-à-dire ici n'excédant pas le chiffre 9 pour la base décimale.

Les résultats intermédiaires référencés 11 à 14 (premier résultat) sont ensuite transformés, par des moyens de calcul de transformation 120, par un algorithme As tiré aléatoirement parmi la pluralité $\underline{s}$, en un deuxième résultat référencé 20 de p chiffres exprimé ici en base décimale

élaboré par une matrice de conversion dans une base décimale mémorisée dans le système de calcul de l'émetteur 1. Le deuxième résultat référencé 20 constitue la première information, d'identification de l'émetteur (IDENT_SPY), utilisée ici ultérieurement pour déterminer la deuxième information (X') et la troisième information (Y').

La première information, d'identification de l'émetteur, IDENT_SPY est ensuite transformée, par des moyens de calcul de cryptage 130, en une autre information ou valeur cryptée référencée 30 ayant un nombre prédéterminé de caractères alphanumériques exprimés dans la base mathématique d'identité Y choisie aléatoirement par l'émetteur 1, par exemple un système de calcul, pour obtenir un identifiant crypté. La base Y est choisie aléatoirement par un algorithme de tirage aléatoire du système de calcul et parmi une pluralité, de taille V, de bases de conversion disponibles mémorisées en association avec le système de calcul. Les V bases de calcul peuvent être comprises, comme dans l'exemple exposé, entre les bases 37 et 67 qui figurent en annexes. Le nombre V de bases peut aussi couvrir la plage entre la base 37 et une base 127, ce qui correspond à un maximum de V = 91 bases, dont la valeur moyenne est 82.

Dans la suite de caractères constituant la valeur cryptée finale référencée 30, des moyens de calcul 140 insèrent, à un rang variable r déterminé de façon aléatoire, le caractère identificateur Y dont la valeur identifie la base de conversion. Le rang r du caractère identificateur Y est fourni par un pointeur Z, encore appelé clé aléatoire, inséré à un rang W prédéterminé ou variable par calcul dans la dite suite cryptée 30.

Lorsque le rang ou position W du pointeur Z est déterminé par calcul, celui-ci est par exemple calculé, par les moyens de calcul 140, en prenant la somme en ASCII d'une ou plusieurs troncatures ou blocs des rubriques

alphanumériques d'une troncature de la chaîne de caractères Ch1 à Ch7 et en déterminant cette somme, modulo 9, dans l'exemple de la base décimale. Le reste ainsi obtenu, par la division par 9, détermine le rang W du pointeur Z, à une étape 41 de la figure 4, et permet donc de le lire, à une étape 42. Dans cet exemple, le pointeur Z est en fait représenté dans la suite cryptée 30 par une adresse en bibliothèque, qui est ainsi lue. Une division du pointeur Z par la valeur s représentative du nombre d'algorithmes As, détermine ensuite, en fin d'étape 42, le rang r du caractère Y d'identification de la base de conversion. La base de conversion Y étant ainsi reconnue et lue à une étape 43, le récepteur 2 peut recalculer en sens inverse, en remontant, la valeur numérique IDENT_SPY en base décimale, à partir du cryptogramme final CRYPT_IDENT après avoir occulté les caractères de service Y et Z, de rangs r et W, à une étape 44. Les références 41 à 44 peuvent aussi représenter les moyens matériels et logiciels assurant les traitements exposés ci-dessus dans le récepteur 2.

Les calculs ou tirages aléatoires effectués par l'un ou l'autre des terminaux émetteur 1 et récepteur 2 peuvent toutefois être pris en charge en tout ou partie par une carte à puce, ou tout autre dispositif de calcul proche ou distant, communiquant avec le terminal considéré. Le terminal, fixe ou portable, et la carte à puce ou autre sont pourvus des algorithmes et des informations mémorisées nécessaires pour amorcer la mise en œuvre de l'une des étapes du processus. Par exemple, la carte à puce peut contenir les tables de conversion et fournir les valeurs nécessaires au terminal.

La carte à puce peut aussi contenir les moyens de tirage aléatoire d'un algorithme parmi la pluralité s et/ou de la table de conversion de la pluralité V. La carte à puce peut également contenir les algorithmes de décryptage pour

obtenir l'information d'identification d'émetteur IDENT_SPY ou les algorithmes de cryptage pour déterminer la consistance à partir des chaînes Ch1 à Ch7. La carte à puce peut également contenir les algorithmes de calcul de la consistance X' ou X'' et de la signification Y' ou Y''. Enfin, la carte à puce peut contenir toute combinaison des fonctions ci-dessus.

On comprendra que l'invention n'est nullement limitée au cas particulier des valeurs fournies en exemple, que ce soit la plage des bases de conversion avec la nature précise de leurs caractères, numériques, alphanumériques ou autres, ou encore la valeur des constantes de calcul utilisées et les longueurs respectives ou nombres respectifs de caractères de chacune des troncatures, c'est-à-dire des divers blocs de caractères.

ANNEXE 1

Matrice de la base 37

b37	B10
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9
a	10
b	11
c	12
d	13
e	14
f	15
g	16
h	17
i	18
j	19
k	20
l	21
m	22
n	23
o	24
p	25
q	26
r	27
s	28
t	29
u	30
v	31
w	32
x	33
y	34
z	35
A	36

ANNEXE 2

Matrice de la base 67

b10	b67	b10	b67
0	0	34	y
1	1	35	z
2	2	36	A
3	3	37	B
4	4	38	C
5	5	39	D
6	6	40	E
7	7	41	F
8	8	42	G
9	9	43	H
10	a	44	I
11	b	45	J
12	c	46	K
13	d	47	L
14	e	48	M
15	f	49	N
16	g	50	O
17	h	51	P
18	i	52	Q
19	j	53	R
20	k	54	S
21	l	55	T
22	m	56	U
23	n	57	V
24	o	58	W
25	p	59	X
26	q	60	Y
27	r	61	Z
28	s	62	@
29	t	63	$
30	u	64	£
31	v	65	&
32	w	66	%
33	x		

REVENDICATIONS

1. Procédé de sécurisation de la transmission d'un message d'un émetteur (1) à un récepteur (2), dans lequel l'émetteur élabore et intègre au message une signature pour former un message signé, caractérisé par le fait qu'il comporte les étapes suivantes :

- l'émetteur associe au message signé des informations (IDEM) de contrôle en émission, découlant du message signé selon une loi déterminée, et
- l'émetteur élabore et émet (105), à destination du récepteur, des données représentant le message signé et les informations de contrôle en émission (IDEM),

et le récepteur :

- reçoit les dites données transmises,
- détermine (204) selon ladite loi des informations (IDEM') de contrôle en réception découlant du message reçu, et
- compare (205) les informations de contrôle en réception (IDEM') avec les informations de contrôle en émission (IDEM), pour valider le message reçu en cas de coïncidence.

2. Procédé selon la revendication 1, dans lequel la dite loi met en œuvre une fonction mathématique.

3. Procédé selon l'une des revendications 1 et 2, dans lequel l'émetteur élabore et transmet en outre des informations d'identification de l'émetteur (CRYPT_IDENT ou IDENT_SPY) ayant servi à personnaliser ladite loi, et le récepteur personnalise de même la loi, d'après les informations d'identification de l'émetteur (CRYPT_IDENT ou IDENT_SPY) reçues, pour déterminer les informations de contrôle en réception.

4. Procédé selon l'une des revendications 1 à 3, dans lequel l'émetteur établit la dite loi pour que les informations de contrôle en émission (IDEM) soient représentatives d'au moins un type d'informations choisi parmi le groupe formé par des informations de consistance (X') et des informations de signification du message (Y').

5. Procédé selon les revendication 3 et 4 ensemble, dans lequel les informations de consistance du message (X) sont déterminées par un premier quotient provenant d'une division des informations d'identification de l'émetteur (IDENT_SPY) par un nombre de caractères contenus dans le message.

6. Procédé selon la revendication 5, dans lequel un premier reste obtenu par la dite division est lui-même divisé par un nombre premier, pour obtenir un deuxième quotient et un deuxième reste, le deuxième reste étant ajouté à une constante pour obtenir un nombre de caractères prédéterminé, de consistance du message, après conversion dans une base choisie parmi une pluralité de bases de conversion.

7. Procédé selon la revendication 6, dans lequel le reste du deuxième quotient est divisé par un nombre premier pour obtenir un troisième quotient associé à un troisième reste dont la valeur est ajoutée à une valeur constante, pour obtenir les informations de consistance du message (X').

8. Procédé selon la revendication 7, dans lequel le nombre premier est 46027 et la constante est 4623.

9. Procédé selon l'une des revendications 4 à 8, dans lequel les informations de consistance (X') du message sont représentées par des caractères dont le nombre est inférieur à un seuil représentant un pourcentage déterminé par rapport à une taille des données transmises.

10. Procédé selon une des revendications 3 et 4 ensemble, dans lequel les informations de signification du message (Y') sont déterminées par sommation d'un nombre déterminé de caractères alphanumériques du message, chaque caractère alphanumérique ayant pour valeur le double d'une valeur ASCII représentative du caractère considéré, diminuée d'une valeur ASCII représentative d'un caractère adjacent, la somme résultante servant de diviseur d'un dividende, constitué par les informations d'identification de l'émetteur (IDENT_SPY), pour obtenir les informations de signification du message.

11. Procédé selon l'une des revendications 4 à 10, dans lequel les informations de signification (Y') du message sont représentées par des caractères dont le nombre est inférieur à un seuil représentant un pourcentage déterminé par rapport à une taille des données transmises.

12. Procédé selon l'une des revendications 3 à 11, dans lequel les informations d'identification de l'émetteur (IDENT_SPY) sont obtenues :

par une étape de transcodage de chaînes, de tailles déterminées, de caractères alphanumériques représentant des rubriques à protéger, fournissant un premier ensemble de résultats intermédiaires ayant chacun un nombre déterminé de chiffres, et

une étape de transformation du premier ensemble de résultats intermédiaires, par un algorithme de transformation (As) choisi aléatoirement parmi une pluralité (s) utilisant chacun une base de caractères alphanumériques particulière à l'algorithme considéré, pour obtenir un résultat final (IDENT_SPY) après conversion par une matrice de conversion des caractères de la base alphanumérique de l'algorithme choisi en des caractères à valeurs numériques d'une base prédéterminée.

13. Procédé selon la revendication 12, dans lequel les informations d'identification de l'émetteur (IDENT_SPY) sont transmises sous forme cryptée, en transformant les informations d'identification de l'émetteur, en base déterminée, en un résultat crypté, à nombre déterminé de chiffres exprimés dans une base mathématique (Y) choisie aléatoirement parmi une pluralité (V) de bases de conversion pour obtenir un identifiant crypté de l'émetteur (CRYPT_IDENT) dans lequel des informations (Y), d'identification de la base mathématique choisie, sont insérées à un rang variable (r) spécifié par un pointeur (Z) inséré à un rang (W) pour lequel le récepteur dispose d'informations pour le déterminer.

14. Procédé selon la revendication 13, dans lequel le rang (r) des informations (Y) d'identification de la base mathématique choisie est défini par un quotient entier obtenu par division d'une valeur particulière, associée par une table au pointeur (Z), par un nombre (s) spécifiant la taille de la pluralité d'algorithmes (As).

15. Procédé selon l'une des revendications 13 et 14, dans lequel le rang (W) du pointeur (Z) est inséré à un rang calculé en prenant la somme, modulo 9, de codes ASCII d'un dit résultat intermédiaire représentant++++ des termes spécifiant une fonction mathématique déterminant les informations d'identification de l'émetteur (IDENT_SPY).

16. Procédé selon l'une revendications 14 et 15, dans lequel le récepteur :

- calcule la somme des codes ASCII d'au moins un bloc de données d'une dite rubrique alphanumérique, reçu dans les informations d'identification de l'émetteur,
- exprime la dite somme en modulo 9, pour déterminer le rang (W) du pointeur (Z),
- lit le dit pointeur (Z) reçu, et

- calcule le rang (r) des informations (Y) d'identification de la base mathématique choisie, en divisant la valeur particulière, associée au pointeur (Z), par la valeur (s) représentant la taille de la pluralité d'algorithmes, exprimées en base prédéterminée, et
- exploite les informations cryptées reçues (CRYPT_IDENT) après en avoir éliminé les informations (Y) d'identification de la base mathématique choisie et le pointeur (Z).

17. Procédé selon l'une des revendications 1 à 16, dans lequel les dites données sont transmises au récepteur à travers un système de stockage de données.

18. Procédé selon la revendication 17, dans lequel le récepteur (2) est aussi l'émetteur (1).

19. Système de sécurisation pour la mise en œuvre du procédé de l'une des revendications 1 à 18, comprenant un émetteur (1) associé à un récepteur (2), l'émetteur étant agencé pour élaborer et intégrer au message une signature pour former un message signé, caractérisé par le fait que :

l'émetteur (1) comporte :

- des moyens (103, 104) pour élaborer et associer, au message signé, des informations (IDEM) de contrôle en émission, découlant du message signé selon une loi déterminée, et
- des moyens (105) d'émission, à destination du récepteur (2), de données représentant le message signé et les informations de contrôle en émission (IDEM),

et le récepteur (2) comporte :

- des moyens de réception des dites données transmises,
- des moyens (203, 204) de détermination, selon ladite loi, d'informations de contrôle en réception découlant du message reçu, et
- des moyens (205) de comparaison des informations de contrôle en réception avec les informations de contrôle

en émission (IDEM), pour valider le message reçu en cas de coïncidence.

20. Système de sécurisation selon la revendication 19, dans lequel les moyens d'émission (105) sont en outre commandés par des moyens (103) d'élaboration d'informations d'identification de l'émetteur (CRYPT_IDENT ou IDENT_SPY) ayant servi à personnaliser ladite loi, et le récepteur comporte des moyens de personnalisation de même de la loi, d'après les informations d'identification de l'émetteur (CRYPT_IDENT ou IDENT_SPY) reçues par les moyens de réception, commandant les moyens (204) de détermination des informations de contrôle en réception.

21. Système de sécurisation selon l'une des revendications 19 et 20, dans lequel l'émetteur est agencé (104) pour que la dite loi fasse que les informations de contrôle en émission (IDEM) soient représentatives d'au moins un type d'informations choisi parmi le groupe formé par des informations de consistance et des informations de signification du message.

22. Support de données contenant un ensemble de logiciels de commande d'un système informatique pour la mise en œuvre du procédé de l'une des revendications 1 à 18, l'ensemble de logiciels comportant au moins l'un parmi les deux sous-ensembles suivants :

un premier sous-ensemble, destiné à l'émetteur, contenant un logiciel pour commander au système d'associer au message signé des informations (IDEM) de contrôle en émission, découlant du message signé selon une loi déterminée, et un logiciel pour commander d'élaborer et d'émettre (105), à destination du récepteur, des données représentant le message signé et les informations de contrôle en émission (IDEM),et

un second sous-ensemble, destiné au récepteur, contenant un logiciel de réception des dites données transmises, un

logiciel de détermination (204), selon ladite loi, des informations (IDEM') de contrôle en réception découlant du message reçu, et un logiciel de comparaison (205) des informations de contrôle en réception (IDEM') avec les informations de contrôle en émission (IDEM), pour valider le message reçu en cas de coïncidence.

23. Support de données selon la revendication 22, dans lequel le premier sous-ensemble contient un logiciel d'élaboration et de transmission en outre des informations d'identification de l'émetteur (CRYPT_IDENT ou IDENT_SPY) ayant servi à personnaliser ladite loi, et le second sous-ensemble contient un logiciel de personnalisation de même de la loi, d'après les informations d'identification de l'émetteur (CRYPT_IDENT ou IDENT_SPY) reçues, pour déterminer les informations de contrôle en réception.

24. Support de données selon l'une des revendications 22 et 23, dans lequel la dite loi est établie pour que les informations de contrôle en émission (IDEM) soient représentatives d'au moins un type d'informations choisi parmi le groupe formé par des informations de consistance (X') et des informations de signification du message (Y').

25. Support de données selon l'une des revendications 22 à 24, constitué par une carte à puce.

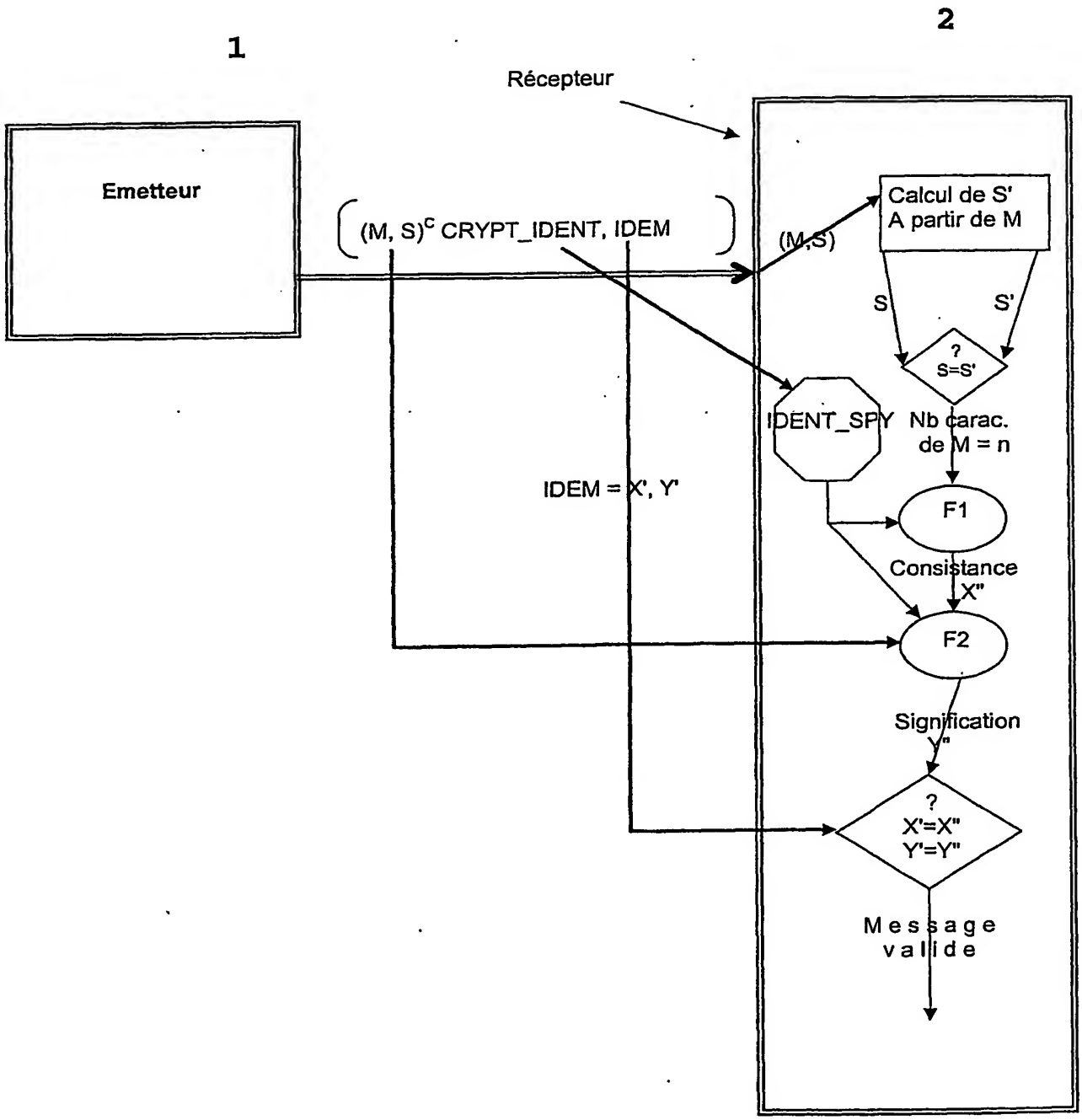

1
2
Récepteur
Emetteur
(M, S)^C CRYPT_IDENT, IDEM
(M,S)
Calcul de S'
A partir de M
S
S'
?
S=S'
IDENT_SPY
Nb carac.
de M = n
IDEM = X', Y'
F1
Consistance
X"
F2
Signification
Y"
?
X'=X"
Y'=Y"
Message
valide

Figure 1

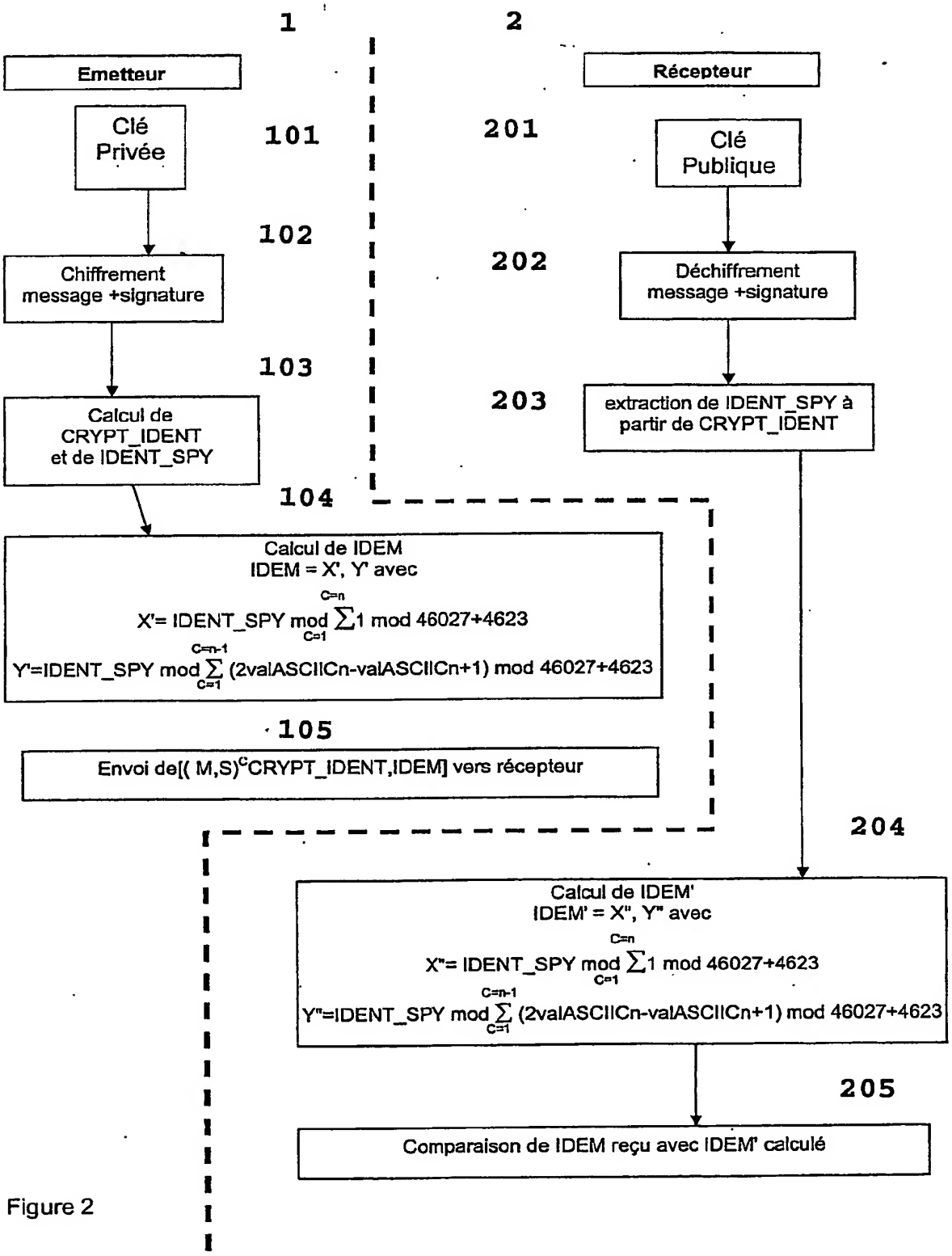

1
2
Emetteur
Récepteur
Clé Privée
101
201
Clé Publique
102
202
Chiffrement message +signature
Déchiffrement message +signature
103
203
Calcul de CRYPT_IDENT et de IDENT_SPY
extraction de IDENT_SPY à partir de CRYPT_IDENT
104
Calcul de IDEM
IDEM = X', Y' avec
X'= IDENT_SPY mod ∑ C=1 à C=n 1 mod 46027+4623
Y'=IDENT_SPY mod ∑ C=1 à C=n-1 (2valASCIICn-valASCIICn+1) mod 46027+4623
105
Envoi de[(M,S)^CCRYPT_IDENT,IDEM] vers récepteur
204
Calcul de IDEM'
IDEM' = X", Y" avec
X"= IDENT_SPY mod ∑ C=1 à C=n 1 mod 46027+4623
Y"=IDENT_SPY mod ∑ C=1 à C=n-1 (2valASCIICn-valASCIICn+1) mod 46027+4623
205
Comparaison de IDEM reçu avec IDEM' calculé

Figure 2

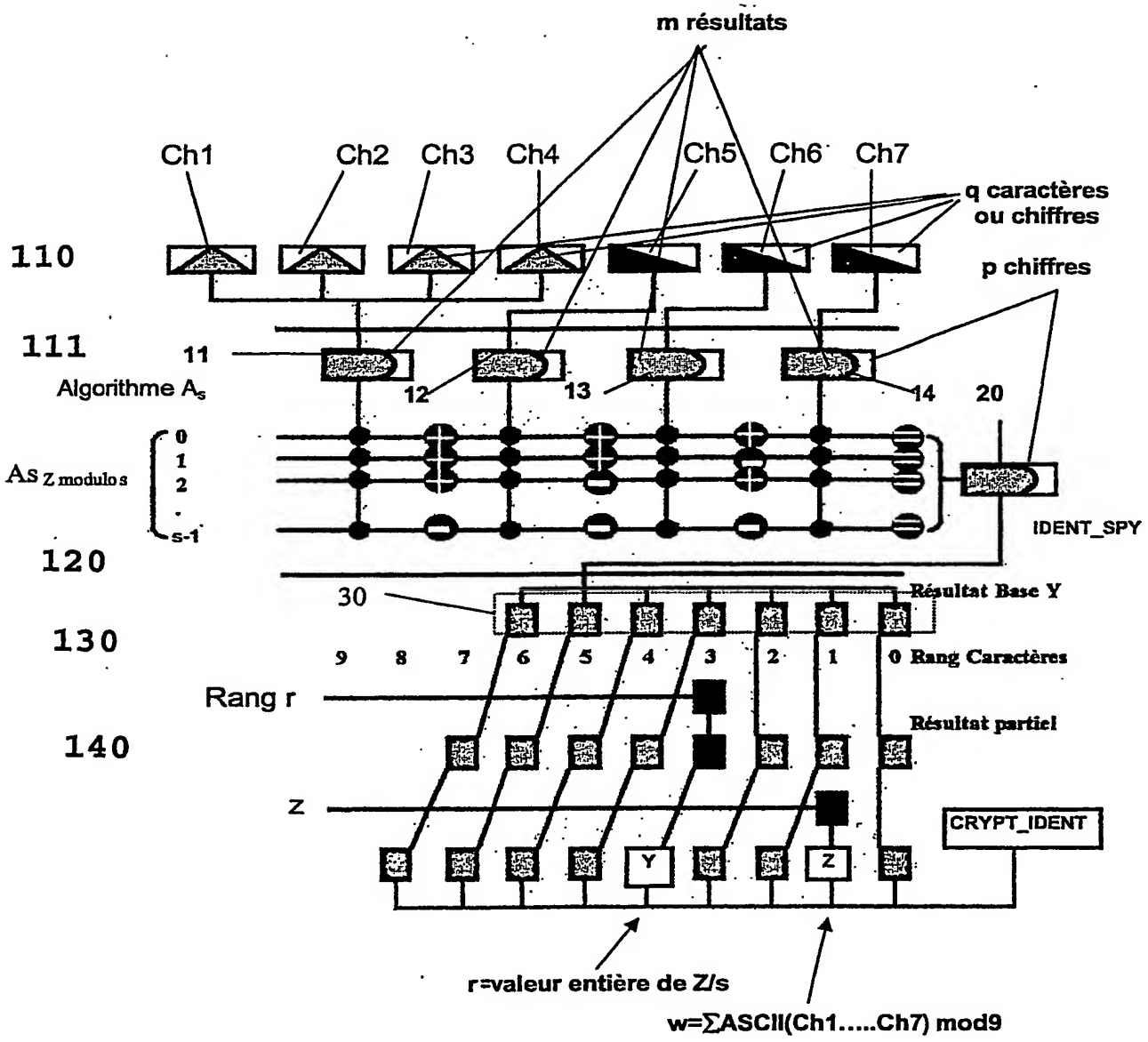
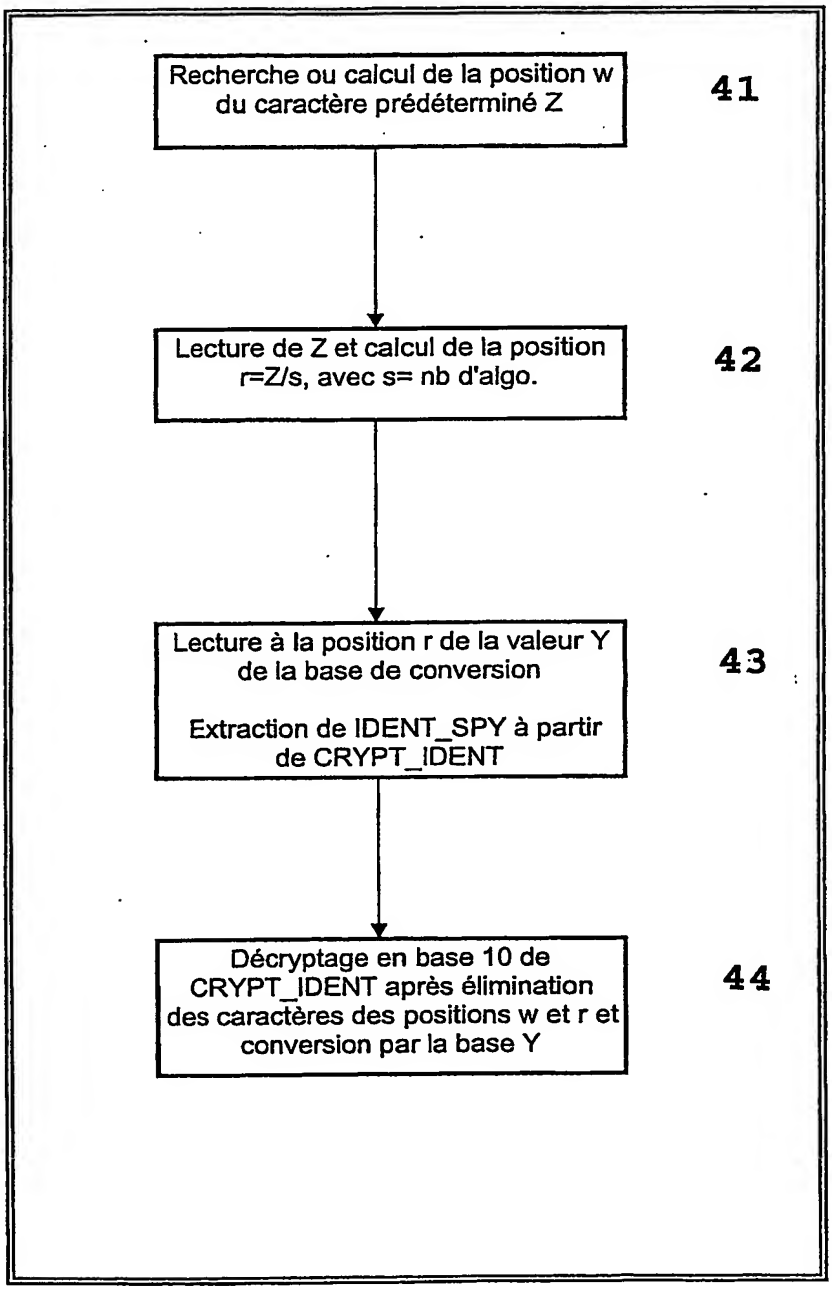

m résultats
Ch1
Ch2
Ch3
Ch4
Ch5
Ch6
Ch7
q caractères ou chiffres
p chiffres
110
111
11
Algorithme A_s
12
13
14
20
$As_{Z \text{ modulo } s}$
0
1
2
s-1
IDENT_SPY
120
30
Résultat Base Y
130
9 8 7 6 5 4 3 2 1 0 Rang Caractères
Rang r
Résultat partiel
140
Z
CRYPT_IDENT
Y
Z
r=valeur entière de Z/s
w=∑ASCII(Ch1.....Ch7) mod9

Figure 3

Figure 4


Recherche ou calcul de la position w du caractère prédéterminé Z
41
Lecture de Z et calcul de la position r=Z/s, avec s= nb d'algo.
42
Lecture à la position r de la valeur Y de la base de conversion
Extraction de IDENT_SPY à partir de CRYPT_IDENT
43
Décryptage en base 10 de CRYPT_IDENT après élimination des caractères des positions w et r et conversion par la base Y
44

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
15 janvier 2004 (15.01.2004)

PCT

(10) Numéro de publication internationale
WO 2004/006498 A3

(51) Classification internationale des brevets[7] : H04L 9/32

(21) Numéro de la demande internationale :
PCT/FR2003/002074

(22) Date de dépôt international : 4 juillet 2003 (04.07.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
02/08418 4 juillet 2002 (04.07.2002) FR

(71) Déposant *(pour tous les États désignés sauf US)* : ERA-COFA SA [FR/FR]; 36, rue du Bois, F-44510 Le Pouliguen (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : SUANEZ, Roger [FR/FR]; 36, rue du Bois, F-44510 Le Pouliguen (FR). ETIENNE, Patricia [FR/FR]; 36, rue du Bois, F-44510 Le Pouliguen (FR).

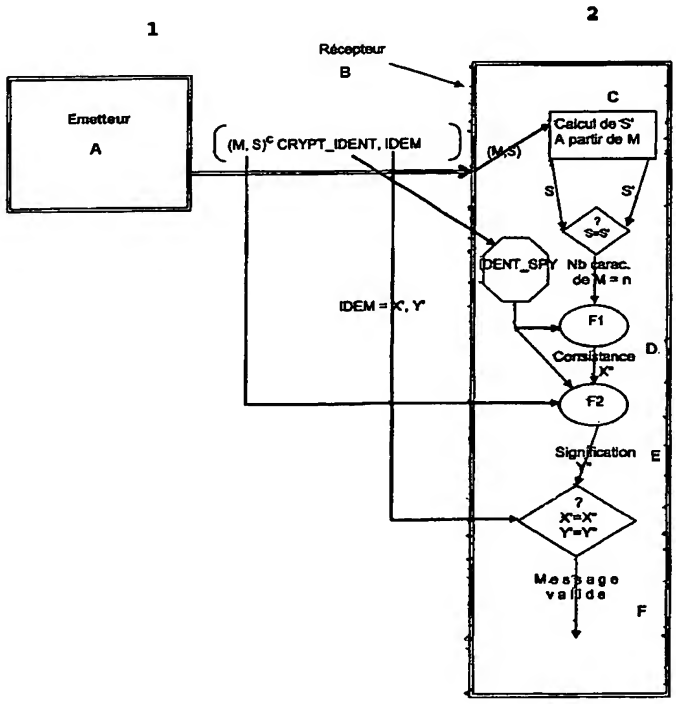
(74) Mandataire : LEPEUDRY, Thérèse; Cabinet Lepeudry, 43, rue de la Brèche aux Loups, F-75012 Paris (FR).

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

[Suite sur la page suivante]

(54) Title: METHOD, SYSTEM AND COMPUTERIZED MEDIUM FOR MAKING SECURE MESSAGE TRANSMISSION

(54) Titre : PROCEDE, SYSTEME ET SUPPORT INFORMATIQUE DE SECURISATION DE TRANSMISSION DE MESSAGES



A...TRANSMITTER
B...RECEIVER
C...CALCULATING NEW SIGNATURE FROM MESSAGE CONTENT
D...CONSISTENCY
E...MEANING
F...VALIDATED MESSAGE

(57) **Abstract:** The invention concerns a method for making secure message transmission comprising a step which consists in transmission of the message and its signature by the transmitter (1) as well as an identification information of the transmitter (CRYPTIDENT) and a supplementary information derived from the message (IDEM), and the receiver (2) likewise determines an information derived from the content of the received message and compares it to the transmitted corresponding information (IDEM) to validate the message in case of conformity.

(57) **Abrégé :** Le procédé de sécurisation de la transmission de message comporte une étape de transmission du contenu du message et de sa signature par l'émetteur (1) ainsi que d'une information d'identification de l'émetteur (CRYPTIDENT) et d'une information supplémentaire découlant du message (IDEM), et le récepteur (2) détermine de même une information découlant du contenu du message reçu et la compare à l'information homologue transmise (IDEM) pour valider le message en cas de coïncidence.

WO 2004/006498 A3

(84) **États désignés** *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *avec rapport de recherche internationale*

(88) **Date de publication du rapport de recherche internationale:** 15 avril 2004

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/[redacted]/02074

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
WPI Data, EPO-Internal, PAJ, IBM-TDB, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2002/023221 A1 (MIYAZAKI KUNIHIKO ET AL) 21 February 2002 (2002-02-21) paragraph '0005!; figures 4,5,15 paragraph '0047! paragraph '0051!	1,17,19
A	paragraph '0063! - paragraph '0064!	2
X	US 6 163 842 A (BARTON JAMES M) 19 December 2000 (2000-12-19) column 1, line 25 - line 43 column 2, line 66 -column 3, line 23 column 4, line 21 - line 35 column 6, line 55 -column 7, line 32 column 7, line 55 - line 64 column 9, line 64 -column 10, line 10	1,2,17, 19

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 December 2003	19/12/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Holper, G

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	DAVIES & W PRICE D: "SECURITY FOR COMPUTER NETWORKS" 1989 , SECURITY FOR COMPUTER NETWORKS. INTRODUCTION TO DATA SECURITY IN TELEPROCESSING AND ELECTRONIC FUNDS TRANSFER, CHICHESTER, WILEY & SONS, GB, PAGE(S) 252-281 XP002150682 page 261, last paragraph -page 262, paragraph 1 ---	1
P,A	WO 02 054667 A (SUANEZ ROGER ;ETIENNE PATRICIA (FR)) 11 July 2002 (2002-07-11) abstract; figure 1 ---	3,23
A	US 6 108 783 A (KRAWCZYK HUGO MARIO ET AL) 22 August 2000 (2000-08-22) column 8, line 31 - line 38; claim 14 -----	3

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2002023221 A1	21-02-2002	AU 758676 B2	27-03-2003
		AU 3887901 A	26-09-2002
		EP 1243999 A2	25-09-2002
		JP 2002335241 A	22-11-2002
		EP 1094424 A2	25-04-2001
		JP 2001331104 A	30-11-2001
US 6163842 A	19-12-2000	US 6115818 A	05-09-2000
		US 5912972 A	15-06-1999
		US 5646997 A	08-07-1997
		US 6523114 B1	18-02-2003
		US 6047374 A	04-04-2000
		US 6101604 A	08-08-2000
WO 02054667 A	11-07-2002	FR 2819068 A1	05-07-2002
		CA 2433224 A1	11-07-2002
		EP 1346512 A1	24-09-2003
		WO 02054667 A1	11-07-2002
US 6108783 A	22-08-2000	NONE	

Demar nationale No

PCT/[illegible]3/02074

A. CLASSEMENT DE L'OBJET DE LA DEMAN

CIB 7 H04L9/32

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)

CIB 7 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

WPI Data, EPO-Internal, PAJ, IBM-TDB, INSPEC

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	US 2002/023221 A1 (MIYAZAKI KUNIHIKO ET AL) 21 février 2002 (2002-02-21) alinéa '0005!; figures 4,5,15 alinéa '0047! alinéa '0051!	1,17,19
A	alinéa '0063! - alinéa '0064!	2
X	US 6 163 842 A (BARTON JAMES M) 19 décembre 2000 (2000-12-19) colonne 1, ligne 25 - ligne 43 colonne 2, ligne 66 -colonne 3, ligne 23 colonne 4, ligne 21 - ligne 35 colonne 6, ligne 55 -colonne 7, ligne 32 colonne 7, ligne 55 - ligne 64 colonne 9, ligne 64 -colonne 10, ligne 10	1,2,17, 19

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
11 décembre 2003	19/12/2003

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Holper, G

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
A	DAVIES & W PRICE D: "SECURITY FOR COMPUTER NETWORKS" 1989 , SECURITY FOR COMPUTER NETWORKS. INTRODUCTION TO DATA SECURITY IN TELEPROCESSING AND ELECTRONIC FUNDS TRANSFER, CHICHESTER, WILEY & SONS, GB, PAGE(S) 252-281 XP002150682 page 261, dernier alinéa -page 262, alinéa 1	1
P,A	WO 02 054667 A (SUANEZ ROGER ;ETIENNE PATRICIA (FR)) 11 juillet 2002 (2002-07-11) abrégé; figure 1	3,23
A	US 6 108 783 A (KRAWCZYK HUGO MARIO ET AL) 22 août 2000 (2000-08-22) colonne 8, ligne 31 - ligne 38; revendication 14	3

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PC[redacted]/02074

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
US 2002023221	A1	21-02-2002	AU	758676 B2	27-03-2003
			AU	3887901 A	26-09-2002
			EP	1243999 A2	25-09-2002
			JP	2002335241 A	22-11-2002
			EP	1094424 A2	25-04-2001
			JP	2001331104 A	30-11-2001
US 6163842	A	19-12-2000	US	6115818 A	05-09-2000
			US	5912972 A	15-06-1999
			US	5646997 A	08-07-1997
			US	6523114 B1	18-02-2003
			US	6047374 A	04-04-2000
			US	6101604 A	08-08-2000
WO 02054667	A	11-07-2002	FR	2819068 A1	05-07-2002
			CA	2433224 A1	11-07-2002
			EP	1346512 A1	24-09-2003
			WO	02054667 A1	11-07-2002
US 6108783	A	22-08-2000	AUCUN		